

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-004225

(43)Date of publication of application : 07.01.2000

(51)Int.Cl.

H04L 9/32  
G06F 15/00  
G09C 1/00

(21)Application number : 10-169698

(71)Applicant : FUJITSU LTD

(22)Date of filing : 17.06.1998

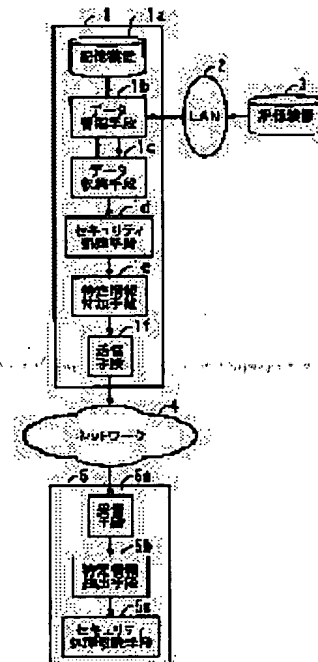
(72)Inventor : TACHIBANA HIROTAKE  
URITA SEICHI  
KOTANI MASATAKE  
HAYASHI TAKEHIKO

## (54) NETWORK SYSTEM, TRANSMISSION/RECEPTION METHOD, TRANSMITTER, RECEIVER AND RECORDING MEDIUM

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To safely transmit data to a called party independently of the skill of an end user or the like.

**SOLUTION:** A data managing means 1b of a transmitter 1 unitarily manages data stored in a storage device 1a or 3. When the transmission of data is requested from terminal equipment not shown in Figure connected to the transmitter 1, a data collecting means 1c collects the desired data while referring to the data managing means 1b. A security processing means 1d performs security processing corresponding to the secrecy level of collected data. A specified information adding means 1e adds specified information for specifying the security processing to data. A transmission means 1f transmits data, to which security processing is performed, through a network 4 to a receiver 5. A reception means 5a of the receiver 5 receives data from the transmitter 1. A specified information extracting means 5b extracts the specified information added to the data. While referring to the specified information, a security processing releasing means 5c releases security processing applied to the data.



### LEGAL STATUS

[Date of request for examination]

29.07.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-4225

(P2000-4225A)

(43)公開日 平成12年1月7日(2000.1.7)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テマコード <sup>*</sup> (参考)
H 0 4 L 9/32		H 0 4 L 9/00	6 7 1 5 B 0 8 5
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 A 5 K 0 1 3
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 E

審査請求 未請求 請求項の数14 O L (全 24 頁)

(21)出願番号 特願平10-169698

(22)出願日 平成10年6月17日(1998.6.17)

(71)出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番  
1号

(72)発明者 橋 博隆

神奈川県川崎市中原区上小田中4丁目1番  
1号 富士通株式会社内

(72)発明者 瓜田 誠一

神奈川県川崎市中原区上小田中4丁目1番  
1号 富士通株式会社内

(74)代理人 100092152

弁理士 服部 毅蔵

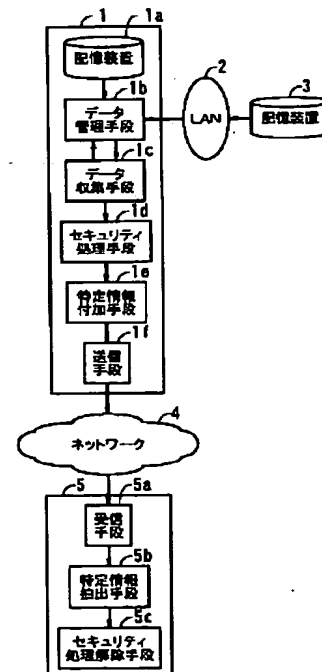
最終頁に続く

(54)【発明の名称】 ネットワークシステム、送受信方法、送信装置、受信装置、および、記録媒体

(57)【要約】

【課題】 セキュリティ処理を統合化する

【解決手段】 送信装置1のデータ管理手段1bは、記憶装置1aまたは記憶装置3に記憶されているデータを一元的に管理する。データ収集手段1cは、送信装置1に接続されている図示せぬ端末装置からデータの送信要求がなされた場合には、データ管理手段1bを参照して所望のデータを収集する。セキュリティ処理手段1dは、収集されたデータの秘匿レベルに応じたセキュリティ処理を施す。特定情報付加手段1eは、セキュリティ処理を特定するための特定情報をデータに付加する。送信手段1fは、ネットワーク4を介して受信装置5にセキュリティ処理が施されたデータを送信する。受信装置5の受信手段5aは送信装置1からのデータを受信する。特定情報抽出手段5bは、データに付加されている特定情報を抽出する。セキュリティ処理解除手段5cは、特定情報を参照してデータに施されているセキュリティ処理を解除する。



## 【特許請求の範囲】

【請求項 1】 送信装置において、データにセキュリティ処理を施した後、受信装置に送信するネットワークシステムにおいて、

送信装置は、

送信しようとするデータにデータ属性、送受信環境から特定されるデータ秘匿レベルに対応するセキュリティ処理を施すセキュリティ処理手段と、

前記セキュリティ処理手段によって施された処理を特定するための特定情報を前記データに対して付加する特定情報付加手段と、

前記特定情報が付加されたデータをネットワークを介して所定の受信装置に対して送信する送信手段と、を有し、

受信装置は、

前記ネットワークを介して伝送されてきたデータを受信する受信手段と、

前記データに付加されている前記特定情報を抽出する特定情報抽出手段と、

前記特定情報を参照して、受信したデータに施されているセキュリティ処理を解除するセキュリティ処理解除手段と、を有することを特徴とするネットワークシステム。

【請求項 2】 前記送信装置は、記憶装置に格納されているデータを一元管理するデータ管理手段と、

前記データ管理手段を参照して、送信しようとするデータを収集するデータ収集手段と、

を更に有することを特徴とする請求項 1 記載のネットワークシステム。

【請求項 3】 前記セキュリティ処理手段は、受信側のアクセス権限レベルも加味してセキュリティ処理を行うことを特徴とする請求項 1 記載のネットワークシステム。

【請求項 4】 前記セキュリティ処理手段は、前記受信装置とネットワークとからなるシステムのシステム安全レベルも加味してセキュリティ処理を行うことを特徴とする請求項 3 記載のネットワークシステム。

【請求項 5】 前記送信装置は、送信しようとするデータのデータ秘匿レベル、ならびに、送信側のアクセス権限レベルおよびシステム安全レベルを与える第 1 のテーブルと、得られたこれら 3 つのレベルをパラメータとして指定されるセキュリティ要素処理の組み合わせとその処理順序とを与える第 2 のテーブルとを更に有し、前記セキュリティ処理手段は、前記第 2 のテーブルより得られたセキュリティ要素処理の組み合わせとその処理順序とに従って、送信しようとするデータに対してセキュリティ処理を施し、

前記特定情報付加手段は、セキュリティ処理が施されたデータに対して、施されたセキュリティ要素処理とその処理順序とを示す情報を特定情報として付加し、

前記特定情報抽出手段は、セキュリティ要素処理とその処理順序とを示す情報を受信したデータから抽出し、前記セキュリティ処理解除手段は、抽出されたセキュリティ要素処理の組み合わせとその処理順序とを示す情報を参照して、セキュリティ処理を解除することを特徴とする請求項 4 記載のネットワークシステム。

【請求項 6】 新たなセキュリティ要素処理を追加するセキュリティ要素処理追加手段を更に有することを特徴とする請求項 5 記載のネットワークシステム。

【請求項 7】 既存のセキュリティ要素処理を更新するセキュリティ要素処理更新手段を更に有することを特徴とする請求項 5 記載のネットワークシステム。

【請求項 8】 前記送信装置および受信装置は、送信しようとするデータのデータ秘匿レベル、ならびに、送信側のアクセス権限レベルおよびシステム安全レベルを与える第 1 のテーブルと、得られたこれら 3 つのレベルをパラメータとして指定されるセキュリティ要素処理の組み合わせとその処理順序とを与える第 2 のテーブルとを更に有し、

前記セキュリティ処理手段は、前記第 2 のテーブルより得られたセキュリティ要素処理の組み合わせとその処理順序とに従って、送信しようとするデータに対してセキュリティ処理を施し、

前記特定情報付加手段は、セキュリティ処理が施されたデータに対して送信元名とデータ名を特定情報として付加し、

前記特定情報抽出手段は、受信したデータから前記送信元名とデータ名とを抽出し、

前記セキュリティ処理解除手段は、抽出された送信元名とデータ名とに対応するセキュリティ要素処理の組み合わせと処理順序を前記第 1 および第 2 のテーブルから取得し、得られたこれらの情報を参照してセキュリティ処理を解除することを特徴とする請求項 4 記載のネットワークシステム。

【請求項 9】 前記送信装置および受信装置の双方がアクセスできるネットワーク上の所定の位置に、送信しようとするデータのデータ秘匿レベル、ならびに、送信側のアクセス権限レベルおよびシステム安全レベルを与える第 1 のテーブルと、得られたこれら 3 つのレベルをパラメータとして指定されるセキュリティ要素処理の組み合わせとその処理順序とを与える第 2 のテーブルとを更に有し、

前記セキュリティ処理手段は、前記第 2 のテーブルより得られたセキュリティ要素処理の組み合わせとその処理順序とに従って、送信しようとするデータに対してセキュリティ処理を施し、

前記特定情報付加手段は、セキュリティ処理が施されたデータに対して送信元名とデータ名を特定情報として付加し、

前記特定情報抽出手段は、前記送信元名とデータ名とを

受信したデータから抽出し、  
前記セキュリティ処理解除手段は、抽出された送信元名とデータ名とに対応するセキュリティ要素処理の組み合わせとその処理順序とを前記第1および第2のテーブルから取得し、得られたこれらの情報を参照してセキュリティ処理を解除することを特徴とする請求項4記載のネットワークシステム。

【請求項10】 送信装置において、データにセキュリティ処理を施した後、受信装置に送信する送受信方法において、

送信装置は、

送信しようとするデータにデータ属性、送受信環境から特定されるデータ秘匿レベルに対応するセキュリティ処理を施し、

施されたセキュリティ処理を特定するための特定情報を前記データに対して付加し、

前記特定情報が付加されたデータをネットワークを介して所定の受信装置に対して送信し、

受信装置は、

前記ネットワークを介して伝送されてきたデータを受信し、

前記データに付加されている前記特定情報を抽出し、前記特定情報を参照して、受信したデータに施されているセキュリティ処理を解除すること、  
ことを特徴とする送受信方法。

【請求項11】 データにセキュリティ処理を施した後、受信装置に対して送信する送信装置において、送信しようとするデータにデータ属性、送受信環境から特定されるデータ秘匿レベルに対応するセキュリティ処理を施すセキュリティ処理手段と、  
前記セキュリティ処理手段によって施された処理を特定するための特定情報を前記データに対して付加する特定情報付加手段と、  
前記特定情報が付加されたデータをネットワークを介して所定の受信装置に対して送信する送信手段と、  
を有することを特徴とする送信装置。

【請求項12】 データにセキュリティ処理を施した後、受信装置に対して送信する送信処理をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体において、  
コンピュータを、  
送信しようとするデータにデータ属性、送受信環境から特定されるデータ秘匿レベルに対応するセキュリティ処理を施すセキュリティ処理手段、  
前記セキュリティ処理手段によって施された処理を特定するための特定情報を前記データに対して付加する特定情報付加手段、  
前記特定情報が付加されたデータをネットワークを介して所定の受信装置に対して送信する送信手段、  
として機能させるプログラムを記録したコンピュータ読

み取り可能な記録媒体。

【請求項13】 送信装置においてセキュリティ処理が施されたデータを受信する受信装置において、  
ネットワークを介して前記送信装置から伝送されてきたデータを受信する受信手段と、  
前記データに付加されている特定情報を抽出する特定情報抽出手段と、  
前記特定情報を参照して、受信したデータに施されているセキュリティ処理を解除するセキュリティ処理解除手段と、  
を有することを特徴とする受信装置。

【請求項14】 送信装置においてセキュリティ処理が施されたデータを受信する受信処理をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体において、  
コンピュータを、  
ネットワークを介して前記送信装置から伝送されてきたデータを受信する受信手段、  
前記データに付加されている特定情報を抽出する特定情報抽出手段、  
前記特定情報を参照して、受信したデータに施されているセキュリティ処理を解除するセキュリティ処理解除手段、  
として機能させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はネットワークシステム、送受信方法、送信装置、受信装置、および、記録媒体に関し、特に、送信装置においてデータにセキュリティ処理を施した後、受信装置に送信するネットワークシステムとその送受信方法、セキュリティ処理を施したデータを送信する送信装置、送信装置でセキュリティ処理が施されたデータを受信する受信装置、セキュリティ処理を施したデータを送信する送信処理をコンピュータに実行させるプログラムを記録した記録媒体、および、送信装置でセキュリティ処理が施されたデータを受信する受信処理をコンピュータに実行させるプログラムを記録した記録媒体に関する。

【0002】

【従来の技術】ネットワークを介してデータを送る場合には、データの漏洩や改竄などを未然に防ぐため、種々のセキュリティ処理（例えば、暗号化処理など）を施したデータを送信する場合が多い。

【0003】

【発明が解決しようとする課題】ところで、ある企業から他の企業に対してデータを送信するような場合には、以下のような手順を踏む必要があった。

(1) 送信側の企業の社内LANなどに分散して格納されている所望のデータを収集する。

(2) 個々のデータの秘匿レベルを、例えば、社内規約などを参照して調べる。

(3) 得られたデータの秘匿レベルに加え、送信時に利用するネットワーク種（専用回線、VAN (Value Added Network)、または、オープンネットワークなど）や送信先のシステム環境などを総合的に考慮して、適用すべきセキュリティ処理を決定する。

(4) 個々のデータに対して、決定されたセキュリティ処理を逐次適用する。

(5) セキュリティ処理の内容を受信側に対して通知する。

(6) セキュリティ処理を施したデータを受信側に対して送信する。

【0004】従って、各プロセスにおいて、以下のような問題点があった。(1)に関しては、所望のデータが格納されている場所を検索し、その場所から手作業でデータを取得する必要があるため、作業が非効率的であるという問題点があった。また、データを物理的にコピーする（ある記録媒体から他の記録媒体にコピーする）ので、同一コンテンツのデータが複数存在することになり、そのため、データの更新時のタイムラグなどによりデータの正当性が保証できない（版数が異なる可能性がある）という問題点があった。(2)に関しては、エンドユーザが個別にデータの秘匿レベルを調査するので、作業が非効率的であり、また、社内規約などを参照して秘匿レベルを主観的に判定することから、セキュリティ処理レベルの統一が困難であるという問題点があった。更に、秘匿レベルの社内規約などが変更された場合には、その通達に時間を要することから、最悪の場合には重要情報が外部に漏れる可能性があるという問題点があった。(3)に関しては、複数のデータを送信する場合に、作業の煩雑性から、個々のデータ毎にきめ細かくセキュリティ処理を設定することが困難であるという問題点があった。そのため、一般的に秘匿レベルの一番高いデータに合わせてセキュリティ処理を施すことが多いので、処理が非効率的になる（重要ではないデータに対してもレベルの高いセキュリティ処理を施すことになる）。また、社内規約書だけでは対応しきれないケースに関しては、エンドユーザのスキルに依存することになり、セキュリティ処理の平準化が困難であるという問題点もあった。更に、相手企業との規約が変更されたような場合、新規処理への移行に時間を要するという問題点もあった。(4)に関しては、エンドユーザが必要なセキュリティ処理用のソフトウェアを購入し、セットアップし、また、運用する必要があるため、作業負荷が大きいという問題点があった。また、セキュリティ処理用のソフトウェアはエンドユーザの端末に導入されていることが通例であるため、例えば、ソフトウェアのバージョンアップがなされた場合には、受信側との間でバージョンの不整合が生じ、セキュリティ処理が施されたデータ

を復号できなくなるといった不都合が生じることもあった。更に、新たなソフトウェアが追加されたような場合にも同様の不都合が生じる。更にまた、エンドユーザがセキュリティ処理の処理手順を誤った場合には、処理の効果が著しく減少したり（例えば、暗号化したデータを圧縮しても十分に圧縮できない）、処理自体が無意味になる（例えば、暗号化したデータにウィルス処理を施しても効果は期待できない）。また、エンドユーザがセキュリティ処理を忘れてしまったような場合には、重要な情報が社外に漏洩することになるという問題点もあった。(5)に関しては、例えば、送信されてきたデータを復号するための手続きを忘れてしまったような場合には、データを復号することが不可能になるという問題点があった。また、受信側では、各社毎（または担当者毎）に異なるセキュリティ処理に対応する必要があるため、作業の負担が大きいという問題点もあった。

【0005】本発明はこのような点に鑑みてなされたものであり、エンドユーザの習熟度などに依存することなく、データを安全に送信先に伝送することを可能とするネットワークシステムおよび送受信方法を提供することを目的とする。

【0006】また、本発明は、送信しようとするデータに対してセキュリティ処理を施す場合に、エンドユーザの負担を軽減することを可能とする送信装置を提供することを目的とする。

【0007】更に、送信側で施されたセキュリティ処理を手手を介さずに確実に復号することを可能とする受信装置を提供することを目的とする。

【0008】

【課題を解決するための手段】本発明では上記課題を解決するために、図1に示ように、送信装置1においてデータにセキュリティ処理を施した後、受信装置5に送信するネットワークシステムにおいて、送信装置1は、送信しようとするデータのデータ属性、送受信環境から特定されるデータ秘匿レベルに対応するセキュリティ処理を前記データに施すセキュリティ処理手段1dと、前記セキュリティ処理手段1dによって施された処理を特定するための特定情報を前記データに対して付加する特定情報付加手段1eと、前記特定情報が付加されたデータをネットワーク4を介して所定の受信装置に対して送信する送信手段1fと、を有し、受信装置5は、前記ネットワーク4を介して伝送されてきたデータを受信する受信手段5aと、前記データに付加されている前記特定情報を抽出する特定情報抽出手段5bと、前記特定情報を参照して、受信したデータに施されているセキュリティ処理を解除するセキュリティ処理解除手段5cと、を有することを特徴とするネットワークシステムが提供される。

【0009】ここで、送信装置1のセキュリティ処理手段1dは、送信しようとするデータにデータ属性、送受

信環境から特定されるデータ秘匿レベルに対応するセキュリティ処理を施す。特定情報付加手段 1 e は、セキュリティ処理手段 1 d によって施された処理を特定するための特定情報をデータに対して付加する。送信手段 1 f は、特定情報が付加されたデータをネットワーク 4 を介して所定の受信装置に対して送信する。受信装置 5 の受信手段 5 a は、ネットワーク 4 を介して伝送されてきたデータを受信する。特定情報抽出手段 5 b は、データに付加されている特定情報を抽出する。セキュリティ処理解除手段 5 c は、特定情報を参照して、受信したデータに施されているセキュリティ処理を解除する。

【0010】また、データにセキュリティ処理を施した後、受信装置 5 に対して送信する送信装置 1 において、送信しようとするデータにデータ属性、送受信環境から特定される秘匿レベルに対応するセキュリティ処理を施すセキュリティ処理手段 1 d と、前記セキュリティ処理手段 1 d によって施された処理を特定するための特定情報を前記データに対して付加する特定情報付加手段 1 e と、前記特定情報が付加されたデータをネットワーク 4 を介して所定の受信装置に対して送信する送信手段 1 f と、を有することを特徴とする送信装置が提供される。

【0011】ここで、セキュリティ処理手段 1 d は、送信しようとするデータにデータ属性、送受信環境から特定されるデータ秘匿レベルに対応するセキュリティ処理を施す。特定情報付加手段 1 e は、セキュリティ処理手段 1 d によって施された処理を特定するための特定情報をデータに対して付加する。送信手段 1 f は、特定情報が付加されたデータをネットワーク 4 を介して所定の受信装置に対して送信する。

【0012】更に、送信装置 1 においてセキュリティ処理が施されたデータを受信する受信装置 5 において、ネットワーク 4 を介して前記送信装置 1 から伝送されてきたデータを受信する受信手段 5 a と、前記データに付加されている特定情報を抽出する特定情報抽出手段 5 b と、前記特定情報を参照して、受信したデータに施されているセキュリティ処理を解除するセキュリティ処理解除手段 5 c と、を有することを特徴とする受信装置が提供される。

【0013】ここで、受信手段 5 は、ネットワーク 4 を介して送信装置 1 から伝送されてきたデータを受信する。特定情報抽出手段 5 b は、データに付加されている特定情報を抽出する。セキュリティ処理解除手段 5 c は、特定情報を参照して、受信したデータに施されているセキュリティ処理を解除する。

【0014】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。図 1 は、本発明の原理を説明する原理図である。この図において、送信装置 1 は、記憶装置 1 a、データ管理手段 1 b、データ収集手段 1 c、セキュリティ処理手段 1 d、特定情報付加手段 1 e、およ

び、送信手段 1 f によって構成されている。また、送信装置 1 は、LAN 2 を介して記憶装置 3 と接続されている。

【0015】受信装置 5 は、ネットワーク 4 を介して送信装置 1 と接続されている。受信装置 5 は、受信手段 5 a、特定情報抽出手段 5 b、および、セキュリティ処理解除手段 5 c によって構成されている。

【0016】送信装置 1 の記憶装置 1 a は、例えば、HDD (Hard Disk Drive) などによって構成されており、種々のデータ (送信の対象となるデータ) を記憶している。

【0017】データ管理手段 1 b は、記憶装置 1 a および記憶装置 3 に記憶されているデータを、例えば、論理データベースなどにより一元管理する。データ収集手段 1 c は、送信しようとするデータをデータ管理手段 1 b の論理データベースを参照して収集する。

【0018】セキュリティ処理手段 1 d は、データ収集手段 1 c によって収集されたデータに対して、そのデータ秘匿レベルに対応するセキュリティ処理を施す。特定情報付加手段 1 e は、セキュリティ処理手段 1 d によって施されたセキュリティ処理を特定するための特定情報をデータに対して付加する。

【0019】送信手段 1 f は、特定情報が付加されたデータをネットワーク 4 を介して受信装置 5 に向けて送信する。受信装置 5 の受信手段 5 a は、ネットワーク 4 を介して伝送されてきたデータを受信する。

【0020】特定情報抽出手段 5 b は、データに付加されている特定情報を抽出する。セキュリティ処理解除手段 5 c は、特定情報を参照して、受信したデータに施されているセキュリティ処理を解除する。

【0021】次に、以上の原理図の動作について説明する。いま、送信装置 1 に接続されている端末装置 (図示せず) から、記憶装置 1 a および記憶装置 3 に格納されている所定の情報 (例えば、パーソナルコンピュータの設計情報) を送信する要求がなされたとなると、データ収集手段 1 c は、関連するデータ (例えば、マザーボードの設計情報、ハードディスクドライブの設計情報、および、グラフィックカードの設計情報など) を取得する要求をデータ管理手段 1 b に対して行う。

【0022】データ管理手段 1 b は、例えば、記憶装置 1 a および記憶装置 3 に格納されているデータを論理的に階層化して管理している (例えば、パーソナルコンピュータの設計情報を、ツリー型の階層構造により系統的に管理している) 論理データベース (以下、DB と適宜略記する) を格納しており、データ収集手段 1 c は、この論理 DB を参照して所望のデータを記憶装置 1 a または記憶装置 3 から取得してセキュリティ処理手段 1 d に供給する。

【0023】セキュリティ処理手段 1 d は、データ収集手段 1 c より供給されたデータに付加されているデータ

秘匿レベルを抽出する。即ち、記憶装置 1 a および記憶装置 3 に記憶されているデータには、それぞれのデータの重要度を示すデータ秘匿レベル（その値が高いほど重要な情報であることを示す）が付加されており、セキュリティ処理手段 1 d は、データ収集手段 1 c より供給されたデータに付加されているデータ秘匿レベルを抽出する。

【0024】そして、セキュリティ処理手段 1 d は、抽出したデータ秘匿レベルに対応するセキュリティ処理を個々のデータに対して施す。例えば、データ秘匿レベルが低い場合には、圧縮処理のみを施し、秘匿レベルが高くなるにつれて、暗号化処理や認証処理などを適切な順序で組み合わせて施す。即ち、圧縮処理は暗号化処理の前に施さなければデータの圧縮率が低下するので、これら双方の処理を施す場合には、圧縮処理、暗号化処理の順序で行う。なお、以下では、セキュリティ処理を構成する個々のセキュリティ処理（例えば、暗号化処理、認証処理、および、圧縮処理など）を「セキュリティ要素処理」と適宜記述する。

【0025】特定情報付加手段 1 e は、セキュリティ処理が施されたデータに対して、施されたセキュリティ要素処理の種類とその処理順序を特定するための特定情報を付加する。

【0026】送信手段 1 f は、特定情報が付加されたデータをネットワーク 4 を介して受信装置 4 に向けて送信する。受信装置 5 の受信手段 5 a は、ネットワーク 4 を介して送信装置 1 から伝送されてきたデータを受信し、特定情報抽出手段 5 b に供給する。

【0027】特定情報抽出手段 5 b は、受信手段 5 a から供給されたデータから特定情報を抽出し、データとともにセキュリティ処理解除手段 5 c に供給する。セキュリティ処理解除手段 5 c は、特定情報抽出手段 5 b から供給された特定情報を参照して、送信装置 1 において施されたセキュリティ要素処理の種類とその処理順序とを認知し、その逆の順序でセキュリティ要素処理をデータに対して施す。その結果、データを復号することができる。例えば、圧縮処理と暗号化処理が施されている場合には、暗号の復号処理を施した後、伸長処理を施すことによりもとのデータを得る。

【0028】このようにして復号されたデータは、図示せぬ記憶装置などに格納され、受信装置 5 側のエンドユーザの要求に応じて、表示装置などに表示出力することが可能となる。

【0029】なお、以上の説明では、送信しようとする個々のデータに対して、個別のセキュリティ処理を施すようにしたが、送信しようとするデータのうち、最も高い秘匿レベルを有するデータに合わせて全てのデータにセキュリティ処理を施すようにしてもよい。

【0030】以上に述べたように、本発明では、送信装置 1 側のエンドユーザが所望の情報を送信しようとした

場合には、まず、データ収集手段 1 c が、データ管理手段 1 b に記憶されている論理 DB を参照して所望の情報に関連するデータを自動的に収集する。次に、セキュリティ処理手段 1 d が、収集されたデータに付加されているデータ秘匿レベルに応じて、所定のセキュリティ要素処理を適切な順序で組み合わせてデータに施す。そして、セキュリティ処理が施されたデータは、施されたセキュリティ要素処理の種類とその処理順序を特定するための特定情報が付加されて受信装置 5 に向けて送信される。

【0031】続いて、受信装置 5 では、受信手段 5 a が送信装置 1 から伝送されてきたデータを受信する。特定情報抽出手段 5 b は、受信したデータから特定情報を抽出し、セキュリティ処理解除手段 5 c が特定情報を参照してデータに施されているセキュリティ処理を解除する。

【0032】従って、本発明によれば、送信側のエンドユーザが手作業で必要なデータを収集する必要がなくなるため、作業の効率を向上させることができるとともに、データの正当性が保証される。

【0033】また、送信側のエンドユーザの個別の判断によらず、データの秘匿レベルに応じて自動的にセキュリティ処理が施されるので、セキュリティ処理レベルを平準化することが可能となるとともに、不注意によって重要な情報が外部に漏洩することを防止することができる。

【0034】更に、社内規約などの規約書だけでは判定が困難なデータに対しても的確なセキュリティ処理がなされるので、エンドユーザのスキルに依存しないセキュリティシステムを構築することができる。

【0035】更にまた、セキュリティ要素処理が統合的に管理されているため、例えば、あるセキュリティ要素処理がバージョンアップされた場合は、送信装置 1 に格納されている要素処理のみを変更するだけでよいので、個々のエンドユーザにかかる負担を軽減することができる。

【0036】また、常に最適な順序でセキュリティ要素処理が施されることから、個々の要素処理の効果を最大限に発揮させることが可能となる。更に、特定情報を参照して処理が自動的に実行されることから、処理手続きを別途送信する手間を省略することができるとともに、処理手順を喪失したことによって、データの復号が不可能となることを防止することができる。

【0037】次に、図 2 および図 3 を参照して、本発明の実施の形態の構成例について説明する。図 2 は、本発明の送信装置の実施の形態の構成例を示すブロック図である。この図において、送信装置 10 は、端末装置 22 ~ 24 などから入力された各種のデータを統合的に管理するとともに、端末装置 22 ~ 24 などから所定の情報に対する送信要求がなされた場合には、対応する情報を

10

20

30

40

50

取得してネットワーク30を介して後述する受信装置に向けて送信する。

【0038】表示装置19は、例えば、CRT (Cathode Ray Tube) モニタによって構成されており、送信装置10から出力される画像信号を表示出力する。LAN (Local Area Network) 20は、例えば、イーサネット (Ethernet) などであり、サーバ21および端末装置22~24を相互に接続し、これらの間でデータの授受を可能とする。

【0039】サーバ21は、種々のデータを記憶した記憶装置を具備しており、端末装置22~24または送信装置10の要求に応じてデータを検索し、LAN20を介して要求を行った装置に対して送信する。また、端末装置22~24から所定のデータが入力された場合には、送信装置10を経由して、記憶装置の所定の領域に格納する。

【0040】端末装置22~24は、各エンドユーザが使用するものであり、所望の情報を受信装置に対して送信したり、新たなデータをサーバ21に登録する。ネットワーク30は、例えば、専用回線、VAN、または、オープンネットワーク (例えば、インターネット) などによって構成されている。

【0041】次に、送信装置10の詳細な構成について説明する。送信装置10は、CPU (Central Processing Unit) 11、ROM (Read Only Memory) 12、RAM (Random Access Memory) 13、ドライバ14、HDD 15、IF (Interface) 16、17、および、バス18によって構成されている。

【0042】CPU11は、装置の各部を制御するとともに種々の演算処理を実行する。ROM12は、CPU11が実行する基本的なプログラム (ファームウェア) や各種データなどを記憶している。RAM13は、CPU11が各種演算処理を実行する場合に、演算途中のデータやプログラムなどを一時的に格納する。

【0043】ドライバ14は、CPU11から供給される描画命令に応じた描画処理を行い、得られた画像を画像信号に変換して表示装置19に出力する。HDD15は、論理データベース15a、データ秘匿レベルテーブル15b、アクセス権限レベルテーブル15c、システム安全レベルテーブル15d、セキュリティ設定多次元テーブル15e、および、セキュリティフィルタ管理テーブル15fを有している。また、セキュリティ要素処理を行うソフトウェアなども格納している。

【0044】論理データベース15aは、サーバ21およびその他の記憶装置 (例えば、端末装置22~24に具備されている記憶装置など) に記憶されているデータを、論理的に階層付けて管理している。

【0045】例えば、パーソナルコンピュータのマザーボードに関する情報が図4に示す構造を有しているとする。即ち、マザーボードB-M-01は、F社製のコン

ポーネントB-S-01と、他社製のコンポーネントB-S-02から構成されている。また、コンポーネントB-S-01は、CPU (B-C-00) と電源B-C-10とによって構成されている。更に、コンポーネントB-S-02は、メモリB-C-20とコネクタB-C-30とによって構成されている。

【0046】このような構造を有するパーソナルコンピュータのマザーボードの設計情報を、例えば、サーバ21および他の記憶装置に分散して格納した場合の格納の一様様を図5に示す。この例では、コンポーネントB-S-01に関する情報が、記憶装置60 (例えば、サーバ21の図示せぬ記憶装置) に格納され、コンポーネントB-S-02に関するデータが、記憶装置61、62 (例えば、端末装置22、23) に分散されて格納されている。また、図4では示していないが、CPU (B-C-00)、電源B-C-10、メモリB-C-20、および、コネクタB-C-30は、それぞれコンポーネントB-C-01とB-C-02、B-C-11とB-C-12、B-C-21とB-C-22、および、B-C-31とB-C-32によって構成されている。

【0047】なお、各データの末尾のハッチングを施した部分は、各データの属性情報を示しており、例えば、記録日時、更新日時、および、データサイズなどの情報である。

【0048】図6は、論理データベース15aに格納されている情報であり、図5に示すデータの階層構造を示している。この図において、各四角形内に示されている文字列 (例えば、B-M-01) は、データ名を示しており、記憶装置に格納する場合のファイル名である。また、ハッチングが施されている部分は、属性情報であり、そのデータが格納されている記憶装置やその位置に関する情報が格納されている。

【0049】このように、論理データベース15aは、物理的に分散して格納されている個々のデータの対応関係に関する情報を保有しており、このような情報を参照することにより、上位の階層にある所定の情報を指定した場合にはそれに関連する (階層がそれよりも下の) 情報を特定するとともに、その格納場所を簡単に取得することが可能となる。例えば、送信する情報として、「B-C-10」を指定した場合には、「B-C-11」と「B-C-12」がその下位の情報であり、また、属性情報によりそれらの格納場所を特定することができる。

【0050】図2に戻って、データ秘匿レベルテーブル15bは、図7に示すように、記憶装置に記憶されているデータの秘匿レベルを格納している。図7に示す例では、PC (パーソナルコンピュータ) に関する情報は、マザーボード、HDD、および、その他の情報から構成されており、更にマザーボードに関する情報は、設計書、コスト、および、生産計画から構成されている。この例では、マザーボードの設計書の秘匿レベルは、



“6”であり、コストおよび生産計画に関する情報は、それぞれ“10”および“5”である。この秘匿レベルが高いほど重要な情報であることを示す。

【0051】なお、サーバ21などにデータを格納する場合には、その重要度に応じたデータ秘匿レベルをデータ秘匿レベルテーブル15bに登録する。このような作業は、各セクションの担当者や送信装置10の管理者が一括して行うようにすれば、各データ間の秘匿レベルを標準化することができる。

【0052】図2に戻って、アクセス権限レベルテーブル15cは、図8に示すように送信相手のアクセス権限レベルを格納している。図8の例では、送信相手の企業に対して、部門およびその業務内容に応じてアクセス権限レベルが割り当てられている。

【0053】例えば、F社のA部門は、そのIDが“01”であり、業務として「PC」を担当しているセクションのアクセス権限レベルは、“1”である。また、HDDを担当しているセクションのアクセス権限レベルは、“3”である。なお、このアクセス権限レベルが高いほど、重要な情報をアクセスできることを示している。

【0054】図2に戻って、システム安全レベルテーブル15dは、図9に示すように送信相手のシステムの安全レベルを格納している。図9の例では、送信相手の企業がその部門別に安全レベルを付与されている。なお、「ネット環境」は、ネットワークに対する安全レベルの評価であり、例えば、専用線であるかインターネットであるかによって安全レベルが査定される。「システム環境」は、使用されるコンピュータシステムに対する安全レベルの評価であり、汎用機、UNIX機、パーソナルコンピュータなどに応じて査定される。「運用環境」は、専用オペレータがいるか、または、ルールが明確であるかなどに応じて査定される。「総合環境」は、ネット環境、システム環境、および、運用環境の平均値であり、この値がシステム安全レベルとして利用される。例えば、F社のA部門は、ネット環境は“6”であり、また、システム環境および運用環境はそれぞれ“7”、“5”である。その結果、これらの平均値である総合環境は、“6”(=(6+7+5)/3)となる。なお、この総合環境の値が大きいほど、システムの総合的な安全レベルが高いことを示している。

【0055】なお、平均値ではなく、各環境の査定値に所定の重み係数を乗算し、得られた結果を加算して得られる値を用いるようにしてもよい。そのような構成によれば、各環境の安全レベルが与える影響を正確に反映した値を求めることが可能となる。

【0056】図2に戻って、セキュリティ設定多次元テーブル15eは、図10に示すように、データ秘匿レベル $\alpha$ 、アクセス権限レベル $\beta$ 、および、システム安全レベル $\gamma$ をパラメータとして対応するフィルタを特定す

る。ここで、フィルタとは複数のセキュリティ要素処理を最適な順序で組み合わせたものを指している。このセキュリティ設定多次元テーブル15eの原理について以下に説明する。

【0057】いま、 $\alpha$ 、 $\beta$ 、 $\gamma$ を軸とする直交座標系を考える。データ秘匿レベル $\alpha$ はその値が大きくなるほど重要な情報であることから、 $\alpha$ の値が原点から離れるに従ってレベルの高いセキュリティ処理を施す必要が生じる。

【0058】また、アクセス権限レベル $\beta$ は、その値が大きくなるほど、重要な情報をアクセス可能であることから、値が大きいほど信頼性の高い送信相手である。従って、 $\beta$ の値は原点に近いほどレベルの高いセキュリティ処理を施す必要がある。

【0059】更に、システム安全レベル $\gamma$ は、その値が大きくなるほど送信相手のシステムの信頼性が高いことから、 $\gamma$ の値が原点に近づくほどレベルの高いセキュリティ処理を施す必要がある。従って、 $\alpha$ 、 $\beta$ 、 $\gamma$ 座標系における位置に応じて、データに施すべきセキュリティ処理（フィルタ）を決定するようにすれば、そのデータに最適なセキュリティ処理を選択することが可能となる。

【0060】図10に示すセキュリティ設定多次元テーブル15eでは、 $\alpha$ 、 $\beta$ 、 $\gamma$ 座標系の定義域を8つの互いに独立な領域（互いに重なり合わない領域）に分割し、それぞれの領域と、その領域に最適なセキュリティ処理を示すフィルタNo.とを対応付けている。

【0061】例えば、データ秘匿レベル $\alpha$ が範囲(1 $\leq \alpha < 5$ )内にあり、アクセス権限レベル $\beta$ が範囲(2 $< \beta \leq 6$ )内にあり、また、システム安全レベルが範囲(2 $< \beta \leq 6$ )内にある場合には、表の第1番目の項目であるNo. 1のフィルタが選択されることになる。

【0062】なお、 $\alpha$ 、 $\beta$ 、 $\gamma$ の定義域は、1 $\leq \alpha$ 、 $\beta$ 、 $\gamma \leq 10$ であるが、図10に示すセキュリティ設定多次元テーブル15eでは、 $\alpha \geq 9$ 、 $\beta \leq 2$ 、および、 $\gamma \leq 2$ が除外されている。これは、 $\alpha$ 、 $\beta$ 、 $\gamma$ の何れかがこのような範囲にある場合には、十分なセキュリティが確保できないことから、データの送信を行わないようにするためである。従って、 $\alpha$ 、 $\beta$ 、 $\gamma$ の何れかがこのような範囲にある場合には、データの送信処理が直ちに停止される。

【0063】図2に戻って、セキュリティフィルタ管理テーブル15fは、図11に示すように、各フィルタNo.に対応するセキュリティ要素処理の種類とその処理順序とを管理している。ここで、記号a～fは、図12に示すように、各セキュリティ要素処理の分類（例えば、認証処理、署名処理、・・・）を示しており、また、a～fを更に細分する数字はその処理の処理内容（例えば、分類eに関しては、LHA、COMPRESSION、・・・）を示している。

【0064】次に、本発明の受信装置の実施の形態の構成例について説明する。図3は、本発明の受信装置の構成例を示すブロック図である。なお、この図において図2に示す送信装置と対応する部分には、対応する符号を付してあるのでその説明は省略する。

【0065】受信装置40は、送信装置10とほぼ同様の構成とされているが、HDD45に格納されているテーブルの種類が異なっている。即ち、送信装置10のHDD15に格納されているテーブルから、データ秘匿レベルテーブル15b、アクセス権限レベルテーブル15c、システム安全レベルテーブル15d、セキュリティ設定多次元テーブル15e、および、セキュリティフィルタ管理テーブル15fが除外され、セキュリティ規約テーブル45gが付加されている。

【0066】セキュリティ規約テーブル45gは、送信装置10から送信されたデータに付加されているフィルタNo.を参照して、対応するセキュリティ要素処理とその処理順序とを与えるように構成されている。

【0067】その他の構成は、図2に示す送信装置10と同様であるのでその説明は省略する。次に、図13を参照して図2に示す実施の形態の動作について説明する。

【0068】図13は、図2に示す実施の形態がデータを送信する場合に実行する処理の一例を説明するフローチャートである。このフローチャートが開始されると、以下の処理が実行される。

[S1] CPU11は、ドライバ14に対して所定の描画指令を供給し、図14に示す送信画面を表示装置19に表示させる。

【0069】図14は、この処理の結果、表示装置19に表示される送信画面の一例である。この表示例では、「送信画面」と題されたダイアログボックス70に、送信元設定領域71、送信先設定領域72、および、送信データ設定領域73が表示されている。また、ダイアログボックス70の右上部には、このダイアログボックスのサイズを変更したり設定を終了するためのボタン77～79が表示されている。更に、ダイアログボックス70の右下部には、設定した内容でデータを送信する場合に操作される送信ボタン80と設定内容をキャンセルする場合に操作されるCANCELボタン81とが具備されている。

【0070】送信元設定領域71には、コンボボックス71a～71dが表示されており、それぞれ、送信者名、送信者の所属する部門、その部門のID、および、その部門の業務内容が入力される。

【0071】送信先設定領域72には、コンボボックス72a～72cが表示されており、それぞれ、受信者名、受信者の所属する部門、その部門のIDが入力される。送信データ設定領域73には、リストボックス73aとエディットボックス73bが表示されている。リス

トボックス73aには送信するデータの候補がツリー形式で表示される。なお、この表示は、論理データベース15aを参照して行われる。リストボックス73aの右側には、垂直スクロールバー74～76が表示されており、所望のデータを検索する場合に操作される。

【0072】リストボックス73aにおいて送信対象となるデータを選択すると、選択された内容は送信されるデータとしてエディットボックス73bに表示される。

[S2] CPU11は、図14に示す送信画面において全ての必要項目の入力が終了し、送信ボタン80が操作され場合にはステップS3に進み、それ以外の場合にはステップS2に戻る。

[S3] CPU11は、図14に示す送信画面において入力された送信先に関する情報を取得する。

【0073】図14の例では、受信者として「G社」が入力されており、その部門とIDとして「A部門」および「01」が入力されているので、これらの情報が取得されることになる。

[S4] CPU11は、図14に示す送信画面において入力された送信データ名を取得する。

【0074】図14の例では、エディットボックス73bに表示されている「マザーボード設計書」が送信データ名として取得されることになる。

[S5] CPU11は、ステップS4において取得した送信データ名に対応するデータを論理データベース15aを参照して、サーバ21または他の記憶装置から収集する。

【0075】図14の例では、図5に示すように複数の記憶装置に分散して格納されているマザーボード設計書に関するデータが収集されることになる。

[S6] CPU11は、データ秘匿レベルテーブル15bを参照して、収集したデータの秘匿レベルを取得する。

【0076】いま、図14に示す送信画面において入力されたマザーボードの設計情報は、図7に示すようにその秘匿レベルが、“6”であることから、CPU11は秘匿レベルとして“6”を取得することになる。

[S7] CPU11は、アクセス権限レベルテーブル15cを参照して、送信先のアクセス権限レベルを取得する。

【0077】いま、図14に示す送信画面において入力された送信先（G社のA部門）は、図8に示すようにそのアクセス権限レベルが、“2.1”であることから、CPU11はアクセス権限レベルとして“2.1”を取得することになる。

[S8] CPU11は、システム安全レベルテーブル15dを参照して、送信先のシステム安全レベルを取得する。

【0078】いま、図14に示す送信画面において入力された送信先（G社のA部門）は、図9に示すようにそ

のシステム安全レベル（総合環境）が、“2. 1”であることから、CPU11はシステム安全レベルとして“2. 1”を取得することになる。

【S9】CPU11は、ステップS6～8において取得したデータ秘匿レベル $\alpha$ 、アクセス権限レベル $\beta$ 、および、システム安全レベル $\gamma$ に対応するフィルタNo. を取得する。

【0079】いま、データ秘匿レベル $\alpha=6$ 、アクセス権限レベル $\beta=2. 1$ 、および、システム安全レベル $\gamma=2. 1$ であることから、これを $\alpha$ 、 $\beta$ 、 $\gamma$ 座標系上に★印としてプロットすると図15のようになる。

【0080】この★印は、図10に示すセキュリティ設定多次元テーブルの第5番目に記載されている範囲（ $5 \leq \alpha < 9$ 、 $2 < \beta \leq 6$ 、 $2 < \gamma \leq 6$ ）に含まれている。従って、図14の入力例では、対応するフィルタNo. として“5”が取得されることになる。

【S10】CPU11は、ステップS5において収集したデータに対して、ステップS10において取得したフィルタNo. のセキュリティ処理を施す。

【0081】いま、ステップS9の処理においてフィルタNo. 5が取得されたことから、CPU11は、図11に示すセキュリティフィルタ管理テーブル15.fを参照してフィルタNo. 5に対応するセキュリティ要素処理を特定する。この例では、対応するセキュリティ要素処理として、a-1、b-2、e-1、および、f-1が特定される。具体的には、これらの処理は、図12に示すように、「PC-CARD」、「MD5」、「LHA」、および、「DES」処理である。

【0082】従って、CPU11は、これらの処理を指定された順序でHDD15から読み出し、ステップS5において収集したデータに施す。この処理の概要を示したのが図17である。No. 5のフィルタでは、機能a、b、e、fが選択されているので、これらの機能が“オン”の状態とされ、それ以外の機能c、dはオフの状態とされている。送信しようとするデータは、図の左から右へ進むうちに、セキュリティ要素処理a-1、b-2、e-1、f-1が施される。なお、これらのセキュリティ要素処理は、前述のように最適な順序で配置されているので、効率よくデータにセキュリティ処理を施すことができる。

【S11】CPU11は、セキュリティ処理が施されたデータをIF17に供給し、そこで、データをパケット化させる。

【0083】図18は、パケット化されたデータの一例を示している。この例では、セキュリティ処理されたデータ96の先頭に、ヘッダ90、送信元91、送信先92、データ名93、送信日時94、および、フィルタNo. 95が付加されている。

【0084】ヘッダ90は、通信プロトコルの種類やデータの種別を特定するための情報を含んでいる。送信元

91および送信先92は、送信元と送信先の名称などの情報を含んでいる。データ名93は、セキュリティ処理されたデータ96のデータ名を含んでいる。送信日時94は、このパケットを送信した日時を含んでいる。フィルタNo. 95は、データに施されたセキュリティ処理のフィルタNo. を含んでいる。

【S12】IF17は、パケット化したデータをネットワーク30を介して送信先の受信装置40に向けて送信する。

【0085】ところで、以上では、送信しようとするデータの全てが同一の秘匿レベルである場合について述べたが、例えば、一部の秘匿レベルが異なるデータを送信する場合について以下に説明する。

【0086】いま、図5に示す、複数の記憶装置に分散して記憶されているデータのうち、電源B-C-10の秘匿レベルが“6”から“1”に変更されたとする。図19に秘匿レベルが変更されたデータの一例を示す。この例では、記憶装置60に記憶されているデータの一部（図中2重線で囲繞されている部分）の秘匿レベルが変更されている。また、図20は、階層構造を示す図上において、秘匿レベルが変更されたデータ（図中2重線で囲繞した部分）の位置を示している。

【0087】図21は、図7に示すデータ秘匿レベルテーブル15.bが、電源の秘匿レベルの変更に伴って改訂された場合の一例を示す。この例では、図7の場合と比較して、資料名「設計書」が更に細分化されており、そのうちの電源の秘匿レベルのみが“1”に設定されている。

【0088】このようなデータに対してセキュリティ処理を施す場合、「CPU」、「メモリ」、および、「コネクタ」の秘匿レベルは不変であるので、これらに対しては、前述の場合と同様のセキュリティ処理が施される。

【0089】しかし、「電源」に対しては、その秘匿レベルが“6”から“1”に変更されていることから、 $\alpha$ 、 $\beta$ 、 $\gamma$ の値はそれぞれ（1、2. 1、2. 1）となり、 $\alpha$ 、 $\beta$ 、 $\gamma$ 座標系における位置は図22に示す★印のようになる。

【0090】この★印は、図23に示すように、フィルタNo. 1に対応する範囲（ $1 \leq \alpha < 5$ 、 $2 < \beta \leq 6$ 、 $2 < \gamma \leq 6$ ）に含まれていることから、図13のステップS9では、フィルタNo. として“1”が取得される。

【0091】従って、ステップS10では、「CPU」、「メモリ」、および、「コネクタ」に対応するデータに対しては、前述の場合と同様にNo. 5のフィルタによってセキュリティ処理が施される。一方、「電源」に対応するデータに対しては、No. 1のフィルタによってセキュリティ処理が施される。即ち、No. 1のフィルタは、図11に示すようにセキュリティ処理機

能a, dよりなり、また、その処理内容は図12に示すように、認証処理である「PC-CARD」とウィルス処理である「VACCINE」から構成されるので、図24に示すような手順により、セキュリティ処理が施されることになる。

【0092】即ち、図24に示すように、セキュリティ要素処理a, dのみがオンの状態とされ、その他は全てオフの状態とされているので、図の左側から入力されたデータは、セキュリティ処理機能aに対応する「PC-CARD」とセキュリティ処理機能dに対応する「VA

CCINE」とが施されることになる。

【0093】そして、以上のようにしてセキュリティ処理が施されたデータは、IF17に供給されてそこでパケット化される。このとき、「電源」に対応するデータに対しては、フィルタNo. 95 (図18参照)として“1”が格納され、一方、その他のデータに対しては、“5”が格納されて送信されることになる。

【0094】従って、秘匿レベルが異なるデータをまとめて送信する場合には、それぞれのデータに最適なセキュリティ処理が施されて送信されることになる。また、社内規約の変更などに伴って、所定のデータの秘匿レベルが変更されたような場合には、データ秘匿レベルテーブル15bの内容を変更するだけで、そのデータに施されるセキュリティ処理を即座に変更することができるので、ここのエンドユーザにかかる負担を軽減することが可能となるとともに、重要な情報が社外に漏洩することを防止することができる。

【0095】次に、以上のようにして送信されたデータが受信装置40によって受信される場合の処理について説明する。図25は、図3に示す受信装置40がデータを受信する場合に実行する処理の一例を示すフローチャートである。このフローチャートが開始されると、以下の処理が実行されることになる。

【S21】IF47は、ネットワーク30を介して送信装置10から伝送されてきたパケットを受信し、RAM43またはHDD45に逐次格納する。

【S22】CPU41は、受信処理が終了したか否かを判定し、終了した場合にはステップS23に進み、それ以外の場合にはステップS22に戻る。

【S23】CPU41は、受信したパケットからフィルタNo. を取得する。

【S24】CPU41は、受信したパケットからデータを取得する。

【S25】CPU41は、セキュリティ規約テーブル45gを参照して、ステップS23で取得したフィルタNo. に対応するセキュリティ要素処理をデータに対して順次施し、データに施されているセキュリティ処理を解除する。

【0096】即ち、セキュリティ規約テーブル45gには、図11および図12に示すような情報が格納されて

いるので、CPU41は、このテーブルに記載されている情報を参照して、ステップS23において抽出したフィルタNo. に対応するセキュリティ要素処理の種類とその処理順序を取得する。

【0097】そして、取得した処理順序の逆の順番でセキュリティ要素処理をデータに対して施すことによりもとのデータを得る。例えば、フィルタNo. が“5”である場合には、CPU41は、受信したデータに対して「DES」、「LHA」、「MD5」、および、「PC-CARD」をこの順序で施すことになる。

【0098】このようにしてセキュリティ処理が解除されたデータは、HDD45などに一旦格納された後、表示装置49などに表示して閲覧することが可能となる。次に、送信装置10のセキュリティ設定多次元テーブル15eの設定内容を変更する場合の処理について説明する。

【0099】図26は、図2に示す送信装置10のセキュリティ設定多次元テーブル15eの設定内容を変更する場合に表示される設定画面の表示例である。この表示例では、「設定画面」と題されたダイアログボックス100が表示されている。ダイアログボックス100の右上には、このボックスの表示サイズを変更したり、処理を終了する場合に操作されるボタン101～103が表示されている。

【0100】また、ボックス内の最上部には、設定対象フィルタNo. 設定部104が表示されており、コンボボックスの右端に表示されている矢印ボタンを操作することにより表示されるプルダウンメニューの中から所望の項目を選択することで、設定の対象とするフィルタのNo. を選択することができる。この例では、値“4”が選択されていることから、フィルタNo. 4が設定の対象となる。

【0101】データ秘匿レベルα設定部105では、αの範囲が入力される。この例では、αの下限と上限とに対応するコンボボックスが表示されており、これらのコンボボックスを操作することにより所望の値を選択することが可能となる。この例では、“5”および“9”が選択されている。

【0102】また、アクセス権限レベルβ設定部106には、βの範囲が入力される。更に、システム安全レベルγ設定部107には、γの値が入力される。また、記号「≦」の部分の1回押圧すると、記号「<」が表示される。また、再度押圧すると記号「≦」が再表示される。従って、この部分を適宜押圧することにより所望の記号を選択することができる。

【0103】なお、このようにして入力された範囲が、他のフィルタの範囲と重なっている場合には、設定内容が意味を持たなくなるため、警告を出したり、その値が入力できなくなるようにしてもよい。

【0104】このようにして入力された設定値を、セキ

セキュリティ設定多次元テーブル15eに登録する場合には登録ボタン108を操作する。その結果、CPU11は、設定画面上において入力された設定値を、HDD15のセキュリティ設定多次元テーブル15eの所定の領域に書き込むことになる。

【0105】なお、CANCELボタン109が操作されると、入力された設定値がキャンセルされ、もとのデータ（変更前のデータ）がセキュリティ設定多次元テーブル15eから読み出されて表示される。

【0106】更に、削除ボタン110が操作されると、HDD15のセキュリティ設定多次元テーブル15eに既に登録されているデータのうち、設定対象フィルタNo.によって指定されるデータが削除されることになる。

【0107】以上の処理によれば、セキュリティ設定多次元テーブル15eの設定値を目的に応じて適宜設定することが可能となる。次に、送信装置10のセキュリティフィルタ管理テーブル15fの設定内容を変更する場合の処理について説明する。

【0108】図27は、図2に示す送信装置10のセキュリティフィルタ管理テーブル15fの設定内容を変更する場合に表示される設定画面の表示例である。この表示例では、「設定画面」と題されたダイアログボックス120が表示されている。ダイアログボックス120の右上には、このボックスの表示サイズを変更したり、処理を終了する場合に操作されるボタン121～123が表示されている。

【0109】ダイアログボックス120は、「フィルタ設定画面」と題されたフィルタ設定領域124と「登録／削除画面」と題されたフィルタ登録／削除領域125とから構成されている。

【0110】フィルタ設定領域124においては、セキュリティフィルタ管理テーブル15fの設定内容が設定内容表示領域124aに表示される。所定の設定項目を変更する場合には、設定内容表示領域124aの右端に設けられている垂直スクロールバー126または矢印ボタン127、128、および、下端に設けられている水平スクロールバー129または矢印ボタン130、131を適宜操作して所望の領域を表示させた後、所望の数値を入力または削除することにより、設定内容を変更することができる。

【0111】また、登録／削除領域125においては、各セキュリティ要素処理の処理内容の設定を行うことができる。「分類」と表示されたコンボボックス125aには、セキュリティ要素処理の分類（例えば、認証、署名、圧縮など）が入力される。

【0112】「枝番」と表示されたコンボボックス125bには、セキュリティ要素処理の枝番号（例えば、1、2、・・・）が入力される。なお、この枝番は、図12に示す「No.」に対応している。

【0113】「処理内容」と表示されたコンボボックス125cには、セキュリティ要素処理の内容（例えば、PC-CARD、MD5、W-MARKなど）が入力される。また、その下のコンボボックス125dには、処理内容に関する付記事項などが入力される。

【0114】「運用開始」と表示されたコンボボックス125eには、セキュリティ要素処理の運用が開始される日時（例えば、1999年8月10日 午前10時）が入力される。

【0115】「有効期限」と表示されたコンボボックス125fには、セキュリティ要素処理の運用期限の日時（例えば、2001年8月10日 午前10時）が入力される。

【0116】また、「登録者」と表示されたコンボボックス125gには、セキュリティ要素処理の登録を行った登録者の氏名（例えば、「橋 博隆」など）が入力される。

【0117】このような設定画面において登録された内容を登録する場合には、登録ボタン132を操作する。この登録ボタン132が操作されると、CPU11は、設定画面において入力された情報を取得し、HDD15のセキュリティフィルタ管理テーブル15fの所定の領域に書き込む。その結果、図27に示す設定画面において入力された情報が登録されることになる。

【0118】また、入力した情報を登録せずにキャンセルする場合には、CANCELボタン133を操作すると、CPU11は、入力された情報を消去するとともに、HDD15のセキュリティフィルタ管理テーブル15fから変更前の情報を読み出してダイアログボックス120の所定の位置に表示する。その結果、登録処理を最初から行うことが可能となる。

【0119】更に、登録／削除領域125に表示されている処理内容を削除する場合には、削除ボタン134を操作する。この削除ボタン134が操作されると、CPU11は、登録／削除領域125に表示されている処理内容に対応する処理を、HDD15から削除する。その結果、不要な処理をHDD15から削除することが可能となる。

【0120】なお、コンボボックス125e、125fから入力された運用開始日時と有効期限とを参照して、対応するセキュリティ要素処理を自動的に運用開始または運用停止するようにしてもよい。

【0121】即ち、CPU11は、セキュリティフィルタ管理テーブル15fに登録されているセキュリティ要素処理を実行する場合に、この運用開始日時と有効期限とを参照して、運用期限内である場合のみに対応する要素処理をデータに対して施すようにすればよい。このような構成によれば、セキュリティ要素処理を運用期間に応じて自動的に管理することが可能となる。

【0122】以上に述べたように、本発明によれば、送

信しようとするデータの秘匿レベルのみならず、送信相手のアクセス権限レベルおよびシステム安全レベルも参照してセキュリティ処理を決定するので、総合的な条件に基づいたセキュリティ処理を施すことができる。

【0123】また、セキュリティ要素処理を変更したりバージョンアップする場合などにおいても、送信装置10に登録されているデータを変更するだけで事足りることから、エンドユーザにかかる負担を軽減することができる。

【0124】更に、各記憶装置に格納されているデータは、論理データベース15aによって一元管理されているため、必要なデータを集めたり版数を管理する手間を省くことが可能となる。

【0125】なお、以上の実施の形態においては、個々のデータの秘匿レベルをデータ秘匿レベルテーブル15bに格納するようにしたが、例えば、それぞれのデータに秘匿レベルを付加して記憶装置に記憶するようにしてもよい。

【0126】そのような構成によれば、同一のデータが複数のエンドユーザによって利用された場合においても、セキュリティ処理を均一化することが可能となる。次に、図28を参照して、本発明のネットワークシステムの第2の実施の形態について説明する。

【0127】図28は、本発明のネットワークシステムの第2の実施の形態の受信装置の構成例を示すブロック図である。なお、この図において、図3と対応する部分には同一の符号を付してあるので、その説明は省略する。また、第2の実施の形態の送信装置は、図2の場合と同様の構成とされているのでその説明は省略する。

【0128】この実施の形態では、図3の場合と比較してHDD45に格納されているテーブルが異なっている。即ち、図28に示す実施の形態では、セキュリティ規約テーブル45gが除外され、データ秘匿レベルテーブル45b、アクセス権限レベルテーブル45c、システム安全レベルテーブル45d、セキュリティ設定多次元テーブル45e、および、セキュリティフィルタ管理テーブル45fが新たに追加されている。なお、このHDD45に記憶されているテーブルは、図2に示す送信装置10に記憶されているものと同様の構成とされている。

【0129】次に、第2の実施の形態の動作について説明する。いま、図2に示す送信装置10の端末装置22～24の何れかにより所定のデータの送信要求がなされたとなると、第1の実施の形態と同様の処理が行われ、データにセキュリティ処理が施されることになる。

【0130】セキュリティ処理が施されたデータは、IF17に供給され、そこでパケット化されることになる。第2の実施の形態においては、図29に示すように、図18に示す第1の実施の形態のパケットから、フィルタNo. 95が除外されたパケットが送信される。

【0131】このようなパケットを受信した受信装置40は、まず、パケットに含まれている送信元91、送信先92、および、データ名93を取得する。前述のように、受信装置40のHDD45に格納されているテーブルは、送信装置10のHDD15に記憶されているものと同様であることから、抽出したデータ名93からデータ秘匿レベルを特定し、また、送信元91および送信先92からアクセス権限レベルとシステム安全レベルとを特定する。

【0132】そして、特定されたこれらのレベルをセキュリティ設定多次元テーブル45eおよびセキュリティフィルタ管理テーブル45fに適用することにより、送信側で施されたセキュリティ処理を特定することができる。

【0133】CPU41は、前述のようにして特定されたフィルタNo. のセキュリティ要素処理を、送信側とは逆の順序によりデータに施す。その結果、送信側で施されたセキュリティ処理を解除してもとのデータを得ることができる。

【0134】以上の構成によれば、送信側から受信側に対してフィルタNo. を送信する必要がなくなることから、送信するデータのデータ量を削減することが可能となる。

【0135】次に、図30および図31を参照して、本発明の第3の実施の形態の構成例について説明する。なお、これらの図において、図2および図3と対応する部分には同一の符号を付してあるのでその説明は省略する。

【0136】図30は、本発明の第3の実施の形態の送信装置の構成例を示すブロック図である。この実施の形態においては、図2の場合と比較して、論理データベース15a以外の全てのテーブルがHDD15から除外されている。また、ネットワーク30にサーバ140およびHDD141が新たに追加されている。その他の構成は、図2の場合と同様である。

【0137】また、図31は、本発明の第3の実施の形態の受信装置の構成例を示すブロック図である。この実施の形態においては、図3の場合と比較して、HDD45に格納されているセキュリティ規約テーブル45gが除外されている。また、図30の場合と同様に、ネットワーク30にサーバ140およびHDD141が新たに追加されている。その他の構成は、図3の場合と同様である。

【0138】サーバ140は、送信装置10または受信装置40からの要求に応じてHDD141に記憶されているデータをネットワーク30を介して送信する。HDD141は、セキュリティ処理に関するテーブルを格納している。即ち、HDD141は、図32に示すように、データ秘匿レベルテーブル141b、アクセス権限レベルテーブル141c、システム安全レベルテーブル

141d、セキュリティ設定多次元テーブル141e、および、セキュリティフィルタ管理テーブル141fを格納している。なお、これらのテーブルは、図2に示すHDD15に格納されているものと同様であるのでその説明は省略する。

【0139】次に、以上の実施の形態の動作について説明する。いま、図30に示す、端末装置22~24の何れかにより、所定のデータの送信要求がなされたとすると、CPU11は、HDD15に格納されている論理データベース15aを参照して、対応するデータを記憶装置から取得する。

【0140】そして、CPU11は、ネットワーク30を介してサーバ140から、収集したデータの秘匿レベル、送信先のアクセス権限レベル、および、システム安全レベルとを取得するとともに、これらの値に応じたセキュリティ要素処理とその処理順序を取得する。そして、取得した処理順序に従って、セキュリティ要素処理をデータに施し、IF17に供給する。

【0141】IF17は、セキュリティ処理が施されたデータを図29に示すようなパケットにパケット化して受信装置40に向けて送信する。このようなパケットを受信した受信装置40のCPU41は、パケットから送信元91、送信先92、および、データ名93を抽出し、これらに対応するセキュリティ処理のフィルタNo.をサーバ140から取得する。

【0142】そして、CPU41は、取得したフィルタNo.に対応するセキュリティ要素処理を逆の順序で、セキュリティ処理されたデータ96に対して施すことにより元のデータを得る。

【0143】以上の実施の形態によれば、送信側と受信側のテーブルが共有化されることから、ネットワーク全体のセキュリティ処理の統合化を図ることが可能となる。なお、上記の処理機能は、コンピュータによって実現することができる。その場合、送信装置および受信装置が有すべき機能の処理内容は、コンピュータで読み取り可能な記録媒体に記録されたプログラムに記述されており、このプログラムをコンピュータで実行することにより、上記処理がコンピュータで実現される。コンピュータで読み取り可能な記録媒体としては、磁気記録装置や半導体メモリなどがある。

【0144】市場に流通させる場合には、CD-ROM (Compact Disk Read Only Memory)やフロッピーディスクなどの可搬型記録媒体にプログラムを格納して流通させたり、ネットワークを介して接続されたコンピュータの記憶装置に格納しておき、ネットワークを通じて他のコンピュータに転送することもできる。コンピュータで実行する際には、コンピュータ内のハードディスク装置などにプログラムを格納しておき、メインメモリにロードして実行するようにすればよい。

【0145】

【発明の効果】以上説明したように本発明によれば、送信装置では、送信データにデータ属性、送受信環境から特定されるデータ秘匿レベルに対応したセキュリティ処理を施すとともに、施されたセキュリティ処理を特定する特定情報を付加して送信し、受信装置では、特定情報を参照してセキュリティ処理を解除するようにしたので、複数のエンドユーザによってデータが送信されるような場合においても、平準化されたセキュリティ処理を施すことが可能となる。

【0146】また、エンドユーザの負担を増大させることなく、確実なセキュリティ処理を施すことが可能となる。

【図面の簡単な説明】

【図1】本発明の原理を説明する原理図である。

【図2】本発明の送信装置の第1の実施の形態の構成例を示すブロック図である。

【図3】本発明の受信装置の第1の実施の形態の構成例を示すブロック図である。

【図4】図2に示す実施の形態に格納されているデータの一例を示す図である。

【図5】図2に示す記憶装置に格納されているデータの格納の一態様を示す図である。

【図6】図2に示す論理データベースに格納されている情報の一例を示す図である。

【図7】図2に示すデータ秘匿レベルテーブルに格納されている情報の一例を示す図である。

【図8】図2に示すアクセス権限レベルテーブルに格納されている情報の一例を示す図である。

【図9】図2に示すシステム安全レベルテーブルに格納されている情報の一例を示す図である。

【図10】図2に示すセキュリティ設定多次元テーブルに格納されている情報の一例を示す図である。

【図11】図2に示すセキュリティフィルタ管理テーブルに格納されている情報の一例を示す図である。

【図12】図2に示すセキュリティフィルタ管理テーブルに格納されている他の情報の一例を示す図である。

【図13】図2に示す実施の形態がデータを送信する場合に実行する処理の一例を説明するフローチャートである。

【図14】図13に示すフローチャートが実行された場合に、表示装置に表示される送信画面の表示例である。

【図15】図2に示すセキュリティ設定多次元テーブルの原理を説明する図である。

【図16】図2に示すセキュリティ設定多次元テーブルの原理を説明する図である。

【図17】図2に示す実施の形態において実行されるセキュリティ処理の原理を説明する図である。

【図18】図2に示す実施の形態から送信されるデータの構造の一例を示す図である。

【図19】図5に示すデータの一部分が変更された場合を

示す図である。

【図 20】図 19 に示すデータの論理構造を示す図である。

【図 21】図 19 に示すデータに対応するデータ秘匿レベルテーブルを示す図である。

【図 22】図 2 に示すセキュリティ設定多次元テーブルの原理を説明する図である。

【図 23】図 2 に示すセキュリティ設定多次元テーブルの原理を説明する図である。

【図 24】図 2 に示す実施の形態において実行されるセキュリティ処理の原理を説明する図である。

【図 25】図 3 に示す実施の形態がデータを受信する場合に実行する処理の一例を説明するフローチャートである。

【図 26】図 2 に示すセキュリティ設定多次元テーブルを設定する場合に表示される設定画面の表示例である。

【図 27】図 2 に示すセキュリティフィルタ管理テーブルを設定する場合に表示される設定画面の表示例である。

【図 28】本発明の受信装置の第 2 の実施の形態の構成を示すブロック図である。

【図 29】図 28 に示す実施の形態が受信するデータの

構造を示す図である。

【図 30】本発明の送信装置の第 3 の実施の形態の構成例を示すブロック図である。

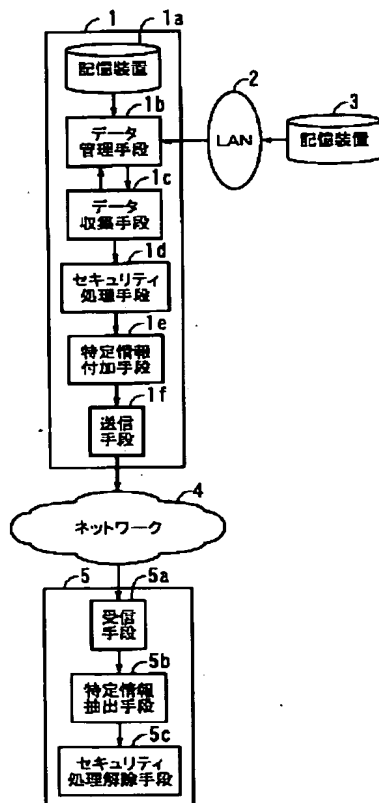
【図 31】本発明の受信装置の第 3 の実施の形態の構成例を示すブロック図である。

【図 32】図 30 に示す実施の形態のサーバに付随する HDD に格納されているデータの一例を示す図である。

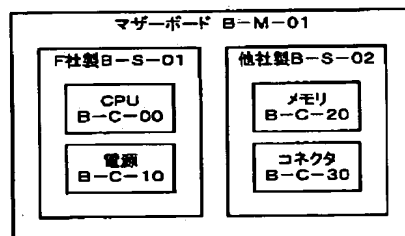
【符号の説明】

- 1 送信装置
- 1 a 記憶装置
- 1 b データ管理手段
- 1 c データ収集手段
- 1 d セキュリティ処理手段
- 1 e 特定情報付加手段
- 1 f 送信手段
- 2 LAN
- 3 記憶装置
- 4 ネットワーク
- 5 受信装置
- 5 a 受信手段
- 5 b 特定情報抽出手段
- 5 c セキュリティ処理解除手段

【図 1】



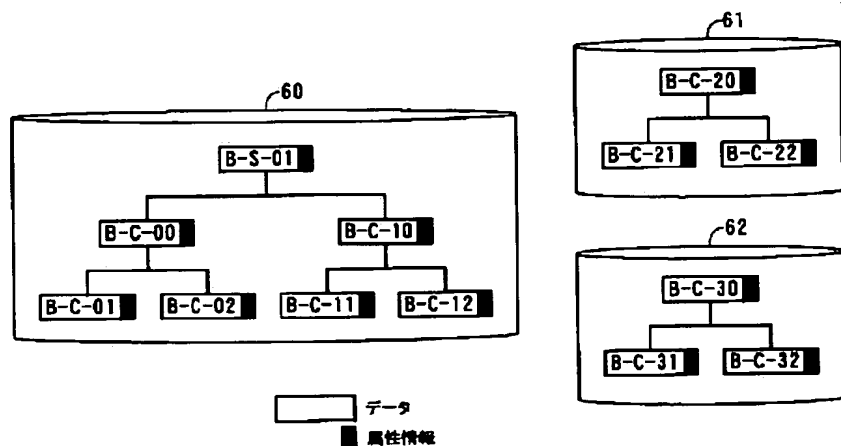
【図 4】



【図 7】

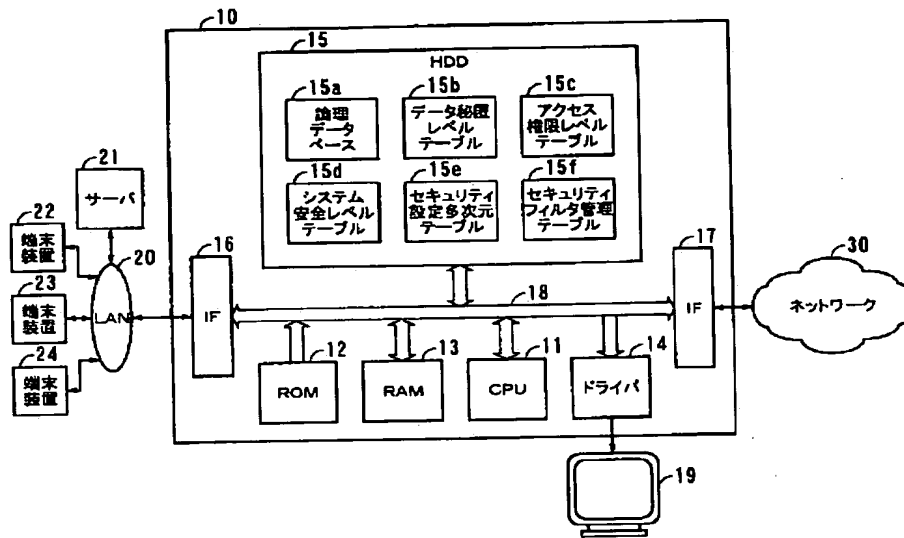
資料名		秘匿レベル
PC	マザーボード	設計書 6
		コスト 10
	生産計画	5
HDD	設計書	7
		...
		...

【図 5】

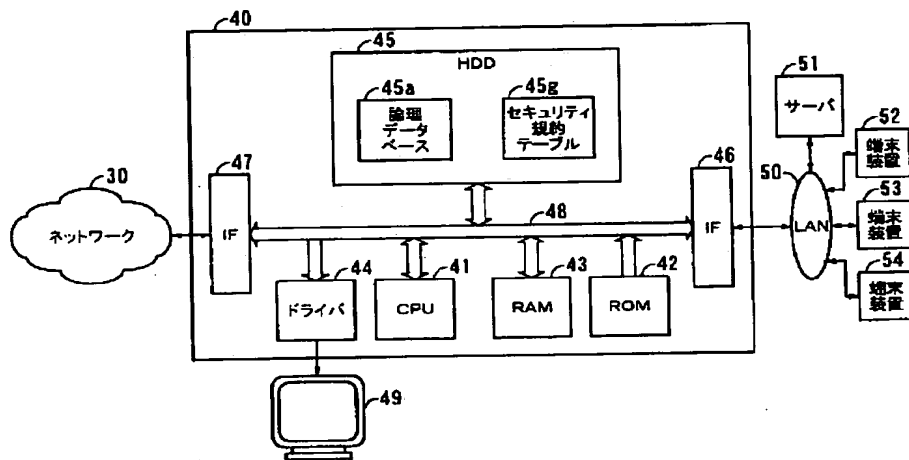




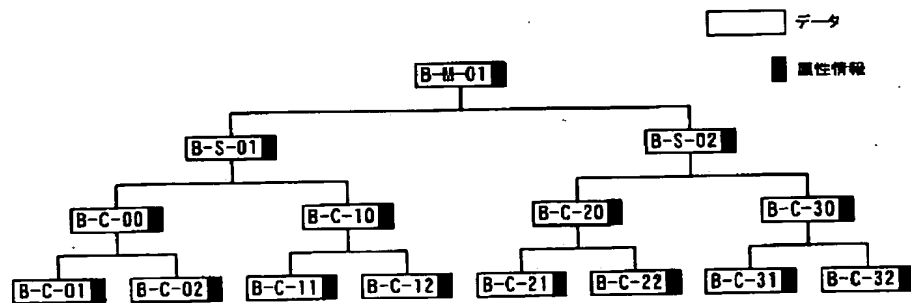
【図2】



【図3】



【図6】



【図8】

企業名	部門	ID	業務	アクセス権限レベル
F社	A部	01	PC	1
			HDD	3
	B部	01	ボード	1.5
G社	A部	01	HDD	2.1
.	.	.	.	.
.	.	.	.	.

【図9】

企業名	部門	ネット環境	システム環境	運用環境	総合環境
F社	A部	6	7	5	6
	B部	4	2	3	3
G社	A部	3	1	2.3	2.1
	B部	6	10	8	8
.	.	.	.	.	.
.	.	.	.	.	.

【図10】

フィルタNo.	データ秘匿レベル $\alpha$	アクセス権限レベル $\beta$	システム安全レベル $\gamma$
1	$1 \leq \alpha < 5$	$2 < \beta \leq 6$	$2 < \gamma \leq 8$
2	$1 \leq \alpha < 5$	$2 < \beta \leq 6$	$6 < \gamma \leq 10$
3	$1 \leq \alpha < 5$	$6 < \beta \leq 10$	$2 < \gamma \leq 6$
4	$1 \leq \alpha < 5$	$6 < \beta \leq 10$	$6 < \gamma \leq 10$
5	$5 \leq \alpha < 9$	$2 < \beta \leq 6$	$2 < \gamma \leq 6$
6	$5 \leq \alpha < 9$	$2 < \beta \leq 6$	$6 < \gamma \leq 10$
7	$5 \leq \alpha < 9$	$6 < \beta \leq 10$	$2 < \gamma \leq 6$
8	$5 \leq \alpha < 9$	$6 < \beta \leq 10$	$6 < \gamma \leq 10$

【図11】

セキュリティ処理機能											
セキュリティ フィルタNo.	a	b	c	d	e				f		...
	1	2	1	1	1	2	3	4	1	2	
1	①			②							
2	①										
3			①		②						
4				①	②						
5	①	②			③				④		
6	①	②				③				④	
7							①		②		
8								①		②	

【図12】

記号	分類	No.	処理内容
a	認証	1	PC-CARD
b	署名	1	PC-CARD
		2	MD5
c	電子すかし	1	W-MARK
d	ウイルス	1	VACCINE
e	圧縮	1	LHA
		2	COMPRESS
		3	GZIP
		4	FLDC
f	暗号	1	DES
		2	RSA
.	.	.	.
.	.	.	.

【図14】

送信画面

送信元

送信先

受信者: 横 博隆

部門: PC設計部

ID: 01

業務: PC設計

受信者: G社

部門: A部門

ID: 01

送信データ

パソコン設計書

マザーボード設計書

CPU(B-C-00)

メモリ(B-C-20)

電源(B-C-10)

コネクタ(B-C-30)

ハードディスク

マザーボード設計書

CPU(B-C-00)

メモリ(B-C-20)

電源(B-C-10)

コネクタ(B-C-30)

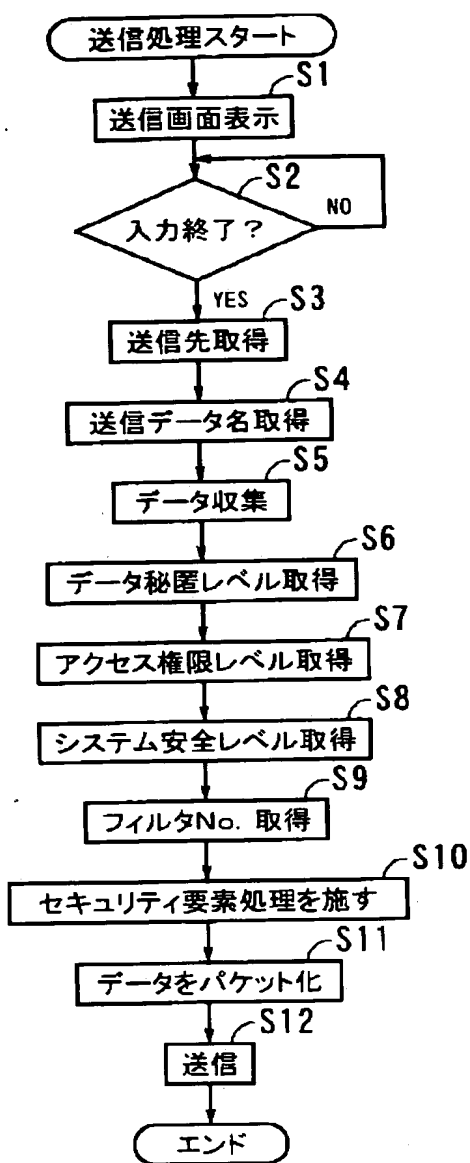
送信

CANCEL

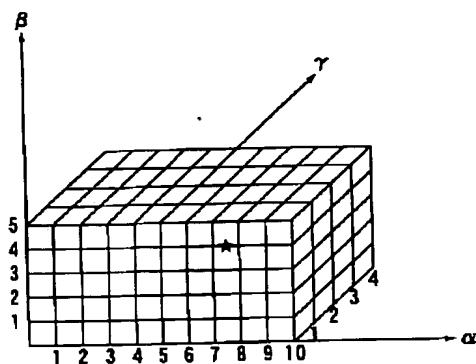
【図18】

90	91	92	93	94	95	96
ヘッダ	送信元	送信先	データ名	送信日時	フィルタNo.	セキュリティ処理されたデータ

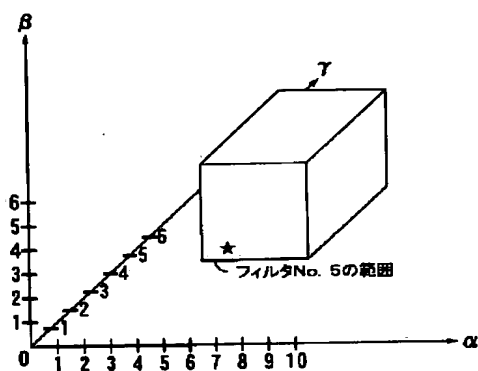
【図13】



【図15】



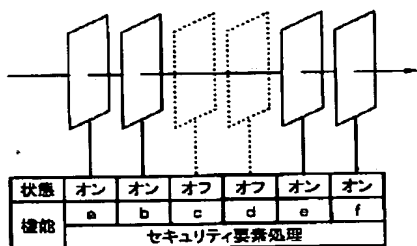
【図16】



【図29】

90	91	92	93	94	96
ヘッダ	送信元	送信先	データ名	送信日時	セキュリティ処理されたデータ

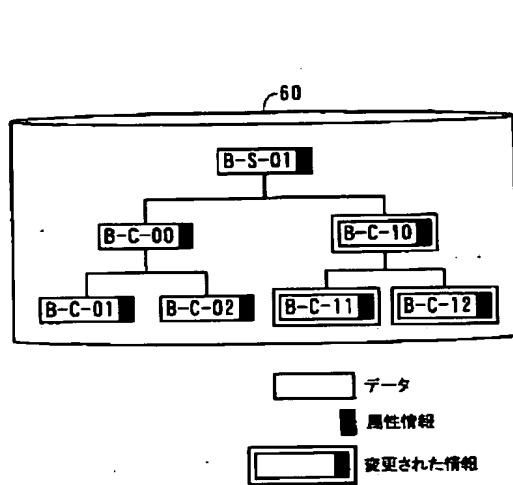
【図17】



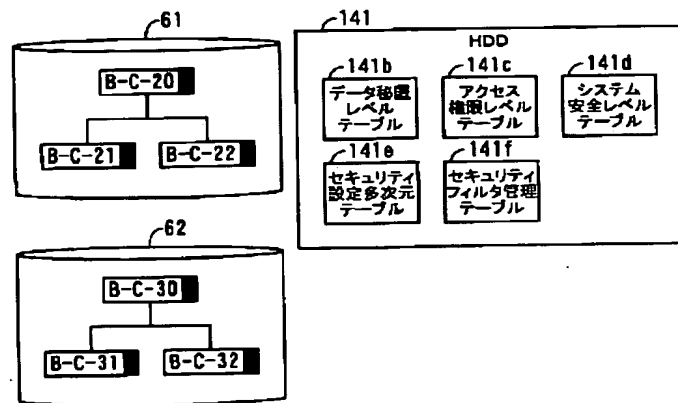
【図21】

資料名		秘匿レベル
PC	マザーボード	設計書
		CPU
		電源
		メモリ
		コネクタ
	コスト	
	生産計画	
HDD	設計書	
	.	
	.	

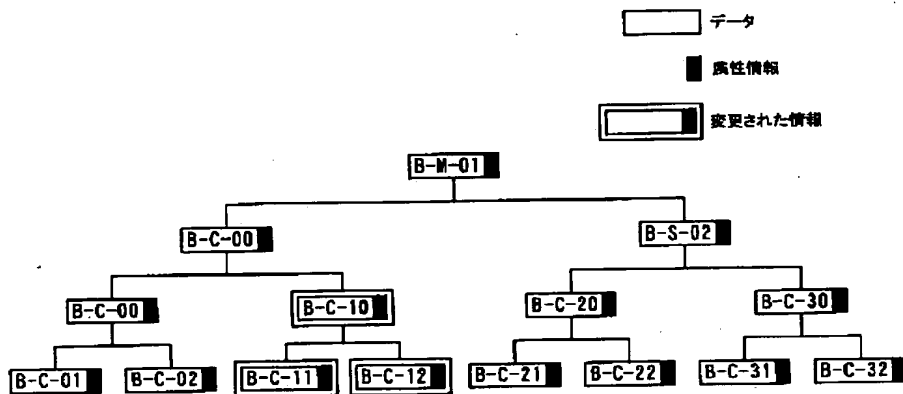
【図 19】



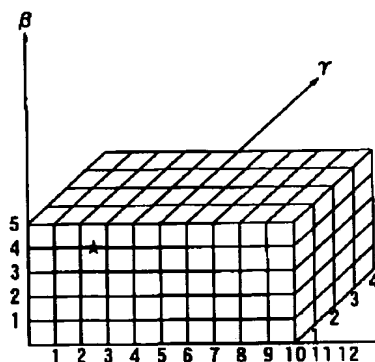
【図 32】



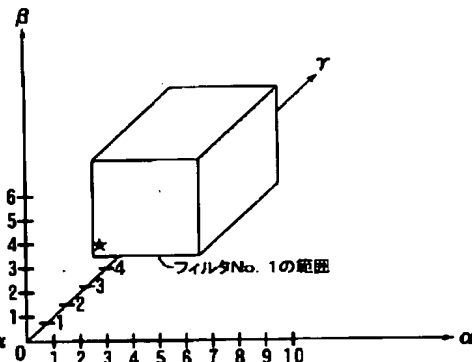
【図 20】



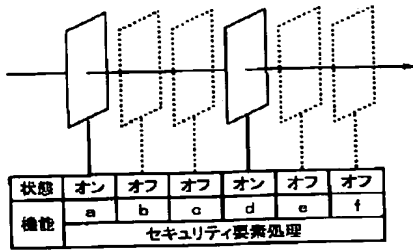
【図 22】



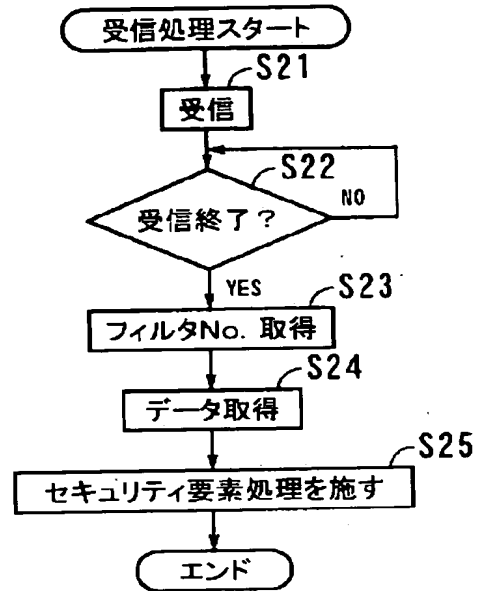
【図 23】



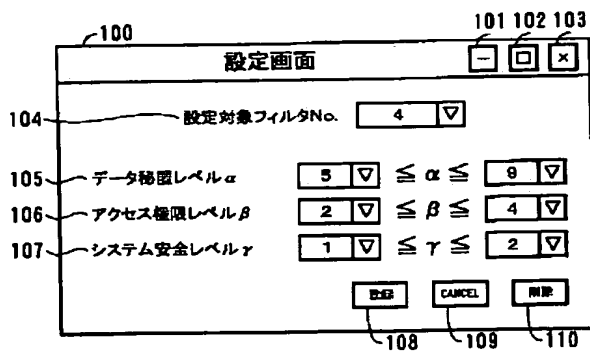
【図24】



【図25】



【図26】



【図27】

設定画面

<フィルタ設定画面>

セキュリティ フィルタNo.	a	b	c	d	e	f	...
1	①			②			
2	①						
3			①	②			
4				①	②		
5	①	②		③		④	
6	①	②			③	④	
7					①	②	
8						①	②

<登録/削除画面>

分類

枝番

処理内容

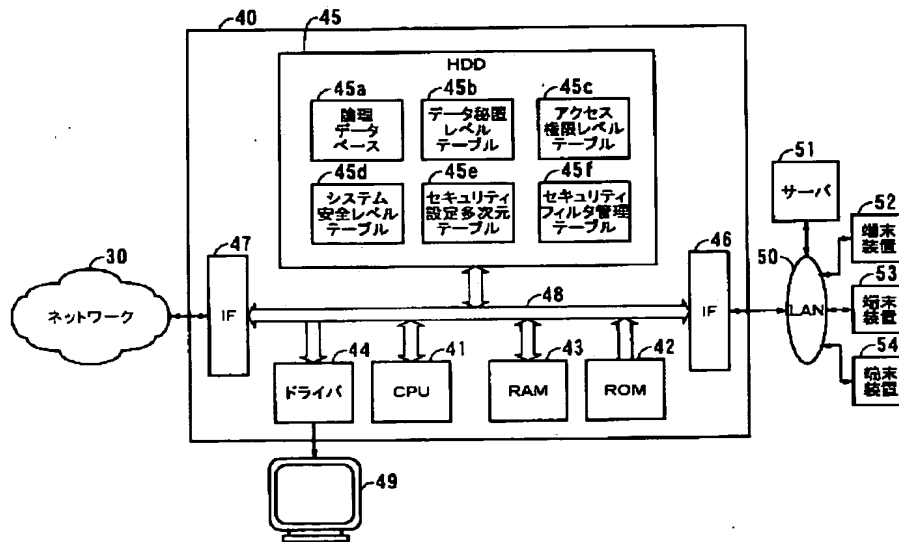
運用開始

有効期限

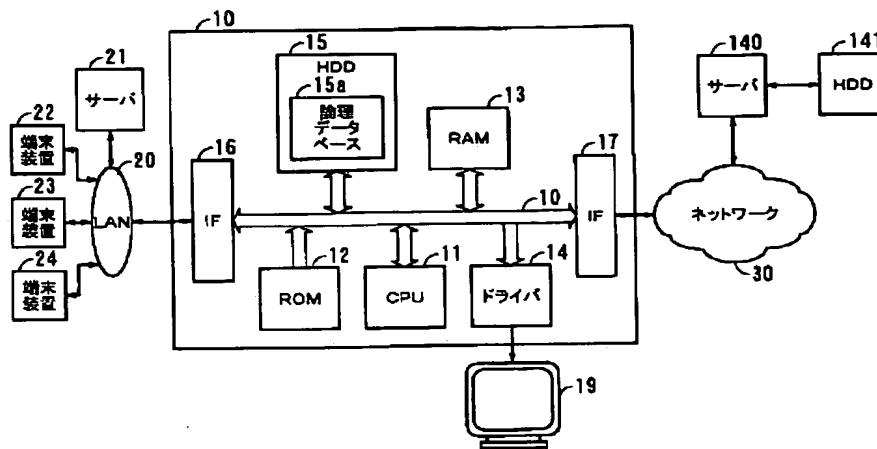
登録者

登録 CANCEL 削除

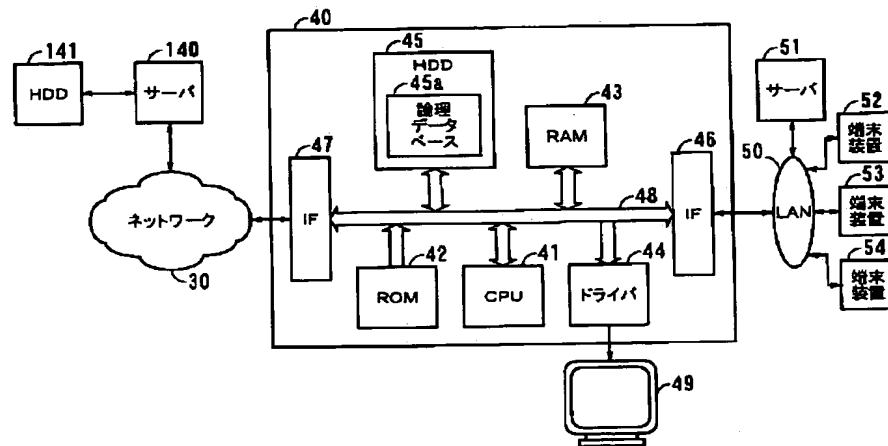
【図28】



【図 30】



【図 31】



## 【手続補正書】

【提出日】平成 11 年 1 月 12 日（1999. 1. 12）

## 【手続補正 1】

【補正対象書類名】明細書

【補正対象項目名】請求項 5

【補正方法】変更

## 【補正内容】

【請求項 5】 前記送信装置は、送信しようとするデータのデータ秘匿レベル、ならびに、受信側のアクセス権限レベルおよびシステム安全レベルを与える第 1 のテーブルと、得られたこれら 3 つのレベルをパラメータとして指定されるセキュリティ要素処理の組み合わせとその処理順序とを与える第 2 のテーブルとを更に有し、

前記セキュリティ処理手段は、前記第 2 のテーブルより得られたセキュリティ要素処理の組み合わせとその処理順序とに従って、送信しようとするデータに対してセキュリティ処理を施し、

前記特定情報付加手段は、セキュリティ処理が施されたデータに対して、施されたセキュリティ要素処理とその処理順序とを示す情報を特定情報として付加し、

前記特定情報抽出手段は、セキュリティ要素処理とその処理順序とを示す情報を受信したデータから抽出し、

前記セキュリティ処理解除手段は、抽出されたセキュリティ要素処理の組み合わせとその処理順序とを示す情報を参照して、セキュリティ処理を解除することを特徴とする請求項 4 記載のネットワークシステム。

## 【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】請求項8

【補正方法】変更

【補正内容】

【請求項8】 前記送信装置および受信装置は、送信しようとするデータのデータ秘匿レベル、ならびに、受信側のアクセス権限レベルおよびシステム安全レベルを与える第1のテーブルと、得られたこれら3つのレベルをパラメータとして指定されるセキュリティ要素処理の組み合わせとその処理順序とを与える第2のテーブルとを更に有し、

前記セキュリティ処理手段は、前記第2のテーブルより得られたセキュリティ要素処理の組み合わせとその処理順序とに従って、送信しようとするデータに対してセキュリティ処理を施し、

前記特定情報付加手段は、セキュリティ処理が施されたデータに対して送信元名とデータ名を特定情報として付加し、

前記特定情報抽出手段は、受信したデータから前記送信元名とデータ名とを抽出し、

前記セキュリティ処理解除手段は、抽出された送信元名とデータ名とに対応するセキュリティ要素処理の組み合わせと処理順序を前記第1および第2のテーブルから取得し、得られたこれらの情報を参照してセキュリティ処理を解除することを特徴とする請求項4記載のネットワークシステム。

## 【手続補正3】

【補正対象書類名】明細書

【補正対象項目名】請求項9

【補正方法】変更

【補正内容】

【請求項9】 前記送信装置および受信装置の双方がアクセスできるネットワーク上の所定の位置に、送信しようとするデータのデータ秘匿レベル、ならびに、受信側のアクセス権限レベルおよびシステム安全レベルを与える第1のテーブルと、得られたこれら3つのレベルをパラメータとして指定されるセキュリティ要素処理の組み合わせとその処理順序とを与える第2のテーブルとを更に有し、

前記セキュリティ処理手段は、前記第2のテーブルより得られたセキュリティ要素処理の組み合わせとその処理順序とに従って、送信しようとするデータに対してセキュリティ処理を施し、

前記特定情報付加手段は、セキュリティ処理が施された

データに対して送信元名とデータ名を特定情報として付加し、

前記特定情報抽出手段は、前記送信元名とデータ名とを受信したデータから抽出し、

前記セキュリティ処理解除手段は、抽出された送信元名とデータ名とに対応するセキュリティ要素処理の組み合わせとその処理順序とを前記第1および第2のテーブルから取得し、得られたこれらの情報を参照してセキュリティ処理を解除することを特徴とする請求項4記載のネットワークシステム。

## 【手続補正4】

【補正対象書類名】明細書

【補正対象項目名】0026

【補正方法】変更

【補正内容】

【0026】送信手段1fは、特定情報が付加されたデータをネットワーク4を介して受信装置5に向けて送信する。受信装置5の受信手段5aは、ネットワーク4を介して送信装置1から伝送されてきたデータを受信し、特定情報抽出手段5bに供給する。

## 【手続補正5】

【補正対象書類名】明細書

【補正対象項目名】0061

【補正方法】変更

【補正内容】

【0061】例えば、データ秘匿レベル $\alpha$ が範囲( $1 \leq \alpha < 5$ )内にあり、アクセス権限レベル $\beta$ が範囲( $2 < \beta \leq 6$ )内にあり、また、システム安全レベルが範囲( $2 < \beta \leq 6$ )内にある場合には、表の第1番目の項目であるNo. 1のフィルタが選択されることになる。

## 【手続補正6】

【補正対象書類名】明細書

【補正対象項目名】0072

【補正方法】変更

【補正内容】

【0072】リストボックス73aにおいて送信対象となるデータを選択すると、選択された内容は送信されるデータとしてエディットボックス73bに表示される。

【S2】CPU11は、図14に示す送信画面において全ての必要項目の入力が終了し、送信ボタン80が操作された場合にはステップS3に進み、それ以外の場合にはステップS2に戻る。

【S3】CPU11は、図14に示す送信画面において入力された送信先に関する情報を取得する。



フロントページの続き

(72)発明者 小谷 誠剛  
神奈川県川崎市中原区上小田中 4 丁目 1 番  
1 号 富士通株式会社内

(72)発明者 林 武彦  
神奈川県川崎市中原区上小田中 4 丁目 1 番  
1 号 富士通株式会社内  
F ターム(参考) 5B085 AE06 AE23 AE29  
5K013 AA02 BA02 EA01 FA03 GA05